IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	
	§	
v.	§	Criminal Action No: 4:24-cr-00298
	§	
EITHAN DAVID HAIM	§	

GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS THE INDICTMENT

TO THE HONORABLE DAVID HITTNER:

The Government respectfully submits this memorandum in opposition to defendant Eithan David Haim's motion to dismiss the indictment (Dkt. No. 91, "Def. Mot."). The defendant asks the Court to dismiss the Government's Superseding Indictment based on a reading of HIPAA's criminal provision that ignores its plain language and context. The result of his interpretation would be both problematic and strange, rendering 42 U.S.C. § 1320d-6 nearly toothless: doctors and health professionals could snoop into the medical records of politicians, celebrities, friends, or strangers who were not their patients without criminal consequences; while only those who broke into a hospital's computer system could be held criminally liable. That is plainly not the meaning of the statute. The Court should deny the motion to dismiss because his legal arguments are meritless, and the rest is a question of fact

for the jury. As set forth below, the Government does not object to striking certain language from Counts Two through Four.

I. LEGAL STANDARD

Motions to Dismiss the Indictment

"[I]t is well settled that an indictment must set forth the offense with sufficient clarity and certainty to apprise the accused of the crime with which he is charged." *United States v. Kay*, 359 F.3d 778, 742 (5th Cir. 2004) (internal quotation marks and citations omitted). "The test for sufficiency is not whether the indictment could have been framed in a more satisfactory manner, but whether it conforms to minimum constitutional standards; namely, that it (1) contain the elements of the offense charged and fairly inform a defendant of the charge against which he must defend, and (2), enable him to plead an acquittal or conviction in bar of future prosecutions for the same offense." *Id.*

When the court decides a motion to dismiss the indictment for failure to state an offense, it is required to "'take the allegations of the indictment as true and to determine whether an offense has been stated.'" *Id.* (quoting *United States v. Hogue*, 132 F.3d 1087, 1089 (5th Cir. 1998)).

A court must deny a motion to dismiss if the motion relies on disputed facts. *See, e.g.*, *United States v. Covington*, 395 U.S. 57, 60 (1969) (holding that a court

can resolve a pretrial motion to dismiss the indictment only when "trial of the facts surrounding the commission of the alleged offense would be of no assistance in determining the validity of the defense"); *United States v. Fontenot*, 665 F.3d 640, 644 (5th Cir. 2011) ("The propriety of granting a motion to dismiss an indictment ... by pretrial motion is by-and-large contingent upon whether the infirmity in the prosecution is essentially one of law or involves determinations of fact.... If a question of law is involved, then consideration of the motion is generally proper.") (citation omitted).

HIPAA

HIPAA provides criminal penalties for the wrongful obtaining or disclosure of individually identifiable health information ("IIHI"). Under 42 U.S.C. § 1320d-6(a),

> A person who knowingly and in violation of this part—
>
> (1) uses or causes to be used a unique health identifier;
>
> (2) obtains individually identifiable health information relating to an individual; or
>
> (3) discloses individually identifiable health information to another person,
>
> shall be punished as provided in subsection (b). For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this

> part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d-9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.

HIPAA's privacy regulation cited in the criminal statute defines a "covered entity" as "(1) A health plan[,] (2) A health clearinghouse[,] [or] (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103. A "transaction" means the "transmission of information between two parties to carry out financial or administrative activities related to health care." *Id.*

As relevant here, HIPAA's criminal provision sets forth different criminal penalties "if the offense is committed under false pretenses," 42 U.S.C. § 1320d-6(b)(2), or "if the offense is committed with intent to sell, transfer, or use individually identifiable health information for . . . malicious harm," *id.* § 1320d-6(b)(3).

II. ARGUMENT

The defendant's motion relies on inapplicable case law to render an otherwise straightforward criminal statute nonsensical. The Court should deny the motion because his legal arguments are meritless, and the rest is a question of fact for the jury.

A. The Court Should Deny the Defendant's Motion to Dismiss the Indictment

The plain language of HIPAA's criminal provision is, as the defense admits, straightforward. As relevant here, Section 1320d-6(a)(2) states that "[a] person who knowingly and in violation of this part . . . obtains individually identifiable health information relating to an individual" shall be punished as set forth in subsection (b). 42 U.S.C. § 1320d-6(a)(2). Subsection (a) goes on to explain that "a person (including an employee or other individual) shall be considered to have obtained . . . . individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d-9(b)(3) of this title) and the individual obtained or disclosed such information without authorization." *Id.*

As drafted, the elements comprising the offense are clear, and there is no need to resort to the HIPAA privacy regulations to understand it. A defendant is guilty if he (a) knowingly and in violation of this part, (b) obtained individually identifiable health information ["IIHI"] relating to an individual maintained by a covered entity without authorization. If he did so under false pretenses, or with intent to use the information for malicious harm, he is subject to enhanced felony penalties. *Id.* § 1320d-6(b).

According to the defendant, the statute "straightforwardly means that the

covered entity maintaining the information must provide 'authorization.'" (Def. Mot. at 11). The Government agrees. "Authorization" is an ordinary word, and may be given its ordinary meaning. Black's Law Dictionary offers one: "Official permission to do something; sanction or warrant." Within the context of the surrounding terms in the statute, "authorization" refers to the permission of the "covered entity" that "maintains" the IIHI. As to whether the defendant obtained the IIHI with or without the authorization, that is not a question of law, but of fact for the jury to determine.

The defendant seeks to circumscribe the meaning of "without authorization" based on dicta in *Van Buren v. United States*, 593 U.S. 374 (2021), a Supreme Court case focused on the Computer Fraud and Abuse Act ("CFAA"), not HIPAA. The holding of *Van Buren* is inapposite here. While the CFAA contains a provision that outlaws access to a computer "without authorization," that provision was not the one at issue in *Van Buren*. Moreover, the Supreme Court's dicta that under the CFAA "without authorization" is a "gates-up-or-down inquiry" makes no sense as applied to HIPAA because, among other reasons, the two statutes are focused on different criminal acts and are drafted differently. (HIPAA was enacted after the CFAA. If Congress had intended the two statutes to work in the same manner, it could have more closely aligned HIPAA with the wording of the CFAA, but it did

not).

Under the CFAA, the illegal act is the unauthorized access of a computer system, leading to the obtaining of certain kinds of information. In contrast, HIPAA's criminal provision is focused on the unauthorized obtaining of the information—not access to a computer or electronic system. Section 1320d-6 contains *no* mention of a computer system or an electronic record system. *Compare* 18 U.S.C. § 1030(a)(2) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information . . ." shall be punished) *with* 42 U.S.C. § 1320d-6 ("[a] person who knowingly and in violation of this part . . . obtains individually identifiable health information relating to an individual" shall be punished). In other words, HIPAA criminalizes the obtaining of the information, not the means by which the defendant does so. As a result, the on/off, access-based definition for authorization proposed by the defendant does not make sense based on HIPAA's language and context, and would improperly circumscribe the meaning of the law. Just because someone *can* obtain a medical record without hacking into an electronic system, does not mean that they are authorized by the hospital to do so.[1]

[1] *Dubin v. United States*, 599 U.S. 110, 124 (2023), also cited by the defendant in a footnote, is likewise inapposite. The identity theft statute at issue there not only

The defendant's interpretation ignores the plain language of the statute and transforms HIPAA's criminal provision into an anti-hacking or anti-break-in statute that absurdly applies only to people like "janitors who access an unlocked EMR terminal and people who scam their way into a hospital data center as a deliveryman to copy records." (Def. Mot. at 13). This flies in the face of common sense and legislative history, which indicates that Congress intended to broadly apply the criminal provision. As the Ninth Circuit noted in *United States v. Huping Zhou*, 678 F.3d 1110, 1114 (9th Cir. 2012), "The House Ways and Means Committee report on [Section 1320d-6] states that 'protecting the privacy of individuals is paramount' and that '[t]his section reflects the Committee's concern than an individual's privacy be protected.'" *Id.* (citing H.R.Rep. No. 104–496(I), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1900, 1903). If the defendant's interpretation were to hold, however, then any person with access to a hospital's EMR system or physical records could look at any medical records they wanted, regardless of whether that person was the patient's caregiver.

The defendant's arguments about the Office of Legal Counsel Memo and subsequent amendment of Section 1320d-6 are off-base, relying on inferences and

---

does not contain the words "without authorization," but the meaning of "without lawful authority" is not addressed by the Supreme Court's decision.

conclusions that do not necessarily follow. (*See* Def. Mot. at 13). Nothing in the OLC memo or the legislative history of the amendment that added "without authorization" suggests that Congress intended to limit the reach of the criminal provision to only those breaking into a hospital, physically or digitally. The defendant's contention that "without authorization" was meant to add liability only to "those who obtain information or disclose IHII but have no authorization to do even that type of task" (Def. Mot. at 13) is unsupported.

The defendant asserts that innumerable problems and "chaos" would arise from hinging authorization on a fact-specific inquiry into the policies and practices of a covered entity. (Def. Mot at 14-15). But these concerns are speculative, overblown, and/or irrelevant. Unlike the CFAA, which touches the lives of most people who use computers, HIPAA does not govern "a breathtaking amount of commonplace . . . activity." *Van Buren*, 593 U.S. at 393. Regarding concerns about uniformity of hospital policies, these issues are speculative and, in any event, the defendant also ignores the fact that all covered entities are governed by the same HIPAA privacy regulations. Hospital policies regarding who can use or disclose patient records and under what circumstances are informed by HIPAA's privacy regulations, ensuring a significant degree of uniformity across institutions. And the alleged problems about whether a defendant needs to receive notice of

hospital policies also do not matter: to be guilty of violating HIPAA's criminal provision, the defendant does not need to know what he did is illegal. *Zhou*, 678 F.3d at 1115 ("42 U.S.C. § 1320d–6(a)(2) is not limited to defendants who knew that their actions were illegal. Rather, the defendant need only know that he obtained individually identifiable health information relating to an individual.").

Finally, the Government disagrees with the defendant's baseless assertion that a trial on "intensely factual questions" with "excruciatingly specific evidence" will simply not work (Def. Mot at 15). Juries routinely consider complex factual issues, such as dueling expert witness interpretations of technical matters, discussions of contract provisions, financial data, accounting principles, and the practices and procedures of institutions like corporations and governmental bodies, to name just a few. The question of whether the defendant had authorization to access the records of patients he was not treating is not so mind-blowingly complex that the criminal process will grind to a halt.

To the extent that the defendant wishes to present evidence that the hospital, in granting him access to its EMR system, thereby authorized him to access patient records of individuals he was not treating, he will have the opportunity to try to do so. It is a fact question for the jury—one that cannot be determined on a motion to dismiss the indictment.

B. A Typo in the Superseding Indictment Does Not Justify Dismissal

The Defendant next argues that, because the indictment mistakenly cites to "Subchapter XL" rather than "Subchapter XI," this requires dismissal. (Def. Mot. at 16-17). However, since the defendant just submitted a 27-page brief discussing HIPAA's criminal provision, there is no question that the defendant has been "apprise[d] . . . of the crime with which he is charged," *Kay*, 359 at 742. A mere typo does not justify dismissing the indictment. *See United States v. Sprick*, 233 F.3d 845, 854 (5th Cir. 2000) ("Clerical or drafting errors . . . which should cause no confusion, do not prejudice the defendant.").

C. The Court May Strike "And/Or Use" From the Superseding Indictment

The defendant then requests that the Court dismiss the indictment, or, in the alternative, strike language from Counts Two through Four that the defendant "did obtain and/or use" IHII. The Government does not object to striking the "and/or use" language to avoid any confusion or potential prejudice.

D. The Court Need Not Reach the Rest of the Defendant's Arguments

The remainder of the defendant's arguments focus on HIPAA's privacy rule as applied to its criminal statutory provision (Def. Mot. at 18-25). While the Government does not concede to any of the arguments that the defendant makes therein, the Court need not reach these issues because, as discussed above, there is no need to import to the privacy rule to understand the meaning of "without authorization."

III. CONCLUSION

For the reasons set forth above, the Court should deny the defendant's motion to dismiss the Superseding Indictment. The Government does not object to striking the "and/or use" language in the Counts Two through Four.

Date: November 5, 2024

Respectfully submitted,

ALAMDAR HAMDANI
United States Attorney
Southern District of Texas

By: *s/*
Tina Ansari
Tyler S. White
Jessica Feinstein
Assistant United States Attorneys
1000 Louisiana Street, 25th Floor
Houston, Texas 77002
Tel.: (713) 567-9000

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this November 5, 2024, I electronically filed the foregoing document with the Clerk of Court using CM/ECF, which will send a notice of electronic filing to all defense counsel of record.

s/ Jessica Feinstein
Jessica Feinstein
Assistant United States Attorney